REMARKS

Claims 1-13 remain pending in the application. Claims 14-20 are newly drafted and will also be pending after entry of this amendment. Applicants respectfully request consideration of all pending claims in light of the remarks presented herein.

Claim Rejections - 35 U.S.C. §102

Claims 1, 2, 9-13 were rejected under 35 U.S.C. § 102(b), as being anticipated by U.S. Patent No. 6,205, 480 to Broadhurst.

Claims 1, 2, 9 and 10

Claims 1, 2, 9 and 10 recite the step of "matching the unique identification (ID) stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers". The Office Action avers that this limitation is taught by Broadhurst in the three passages reproduced below. (Office Action, Page 2, Paragraph 4, Lines 11-13), Page 3, Paragraph 6, Lines 11-13, and Page 4, Paragraph 7 Line 12-14). Applicant respectfully traverses.

> [Passage 1] In step 104, it is determined whether the user already has a cookie containing a network credential. If there is not yet a user cookie, one is created in step 106. (Broadhurst, Column 4, Lines 20-23).
>
> [Passage 2] According to exemplary embodiments, an initial authentication is performed to access a first application via a first server, and the user's identity is mapped onto a network credential which includes a user role. (Broadhurst, Column 2, Lines 33-36).
>
> [Passage 3] To access additional resources not included in the initial list, the user inputs a

request to access additional resources, which may be associated with the user's initial server or new server in the network. (Broadhurst, Column 3, Lines 48-52).

Studying these passages, there is nothing in these passages that discloses or suggests matching a unique ID stored on the client to that stored either on the first or other server when the user communicates with the server.

In fact, the passages teach away from matching a unique ID stored on the client with that on a server. The passages teach that the client either already has a cookie containing authentication information or that the server will create a cookie with authentication information. (Broadhurst, Figure 2 Column 4, Lines 20-23). Since the client either already has a cookie containing authentication information or the server creates a cookie with authentication information, the server does not need to match a unique user ID stored on a client with the unique ID stored on a server to authenticate the client.

On closer examination of the Broadhurst disclosure, Broadhurst proposes controlling (client) access to web server resources through a script written by a system administrator. (Broadhurst, Column 3, Lines 52-56). The script is stored on the web server and provides the login code for server applications. (Broadhurst, Column 3, Lines 55-58). The script does not contain a user name or password. (Broadhurst, Column 3, Lines 58-59). The user name and password is stored in a Script access procedure Variable (SV) under names chosen by the system administrator. (Broadhurst, Column 3, Lines 58-61). To generate the login code, a user requests access (to the server resources) through a browser (on a client). (Broadhurst, Column 3, Lines 66-67). In response to the request, the server script retrieves the SV from a directory 16 based on the SV name in the script, as well as the user's role and the identity contained in a cookie. (Broadhurst, Column 3, Line 67- Column 4, Line 3). This completes the authentication procedure. Notably, Broadhurst authentication procedure does not include matching a unique ID stored on the client with that stored on a server.

Broadhurst's authentication procedure requires scripts, secure access variables, browsers and cookies. This procedure is a far cry from Applicants' recited invention. In contrast, Applicants' method (computer system) matches a unique ID stored on a client with that on a

server providing an elegant solution for client authentication without the need for cookies. Notably, Applicants' method does not require servers that run scripts to access secure access variables and generate cookies. Moreover, Applicants' method does not require clients that support browsers and cookies.

Claims 11-13

Claims 11-13 recite "a server computer running a server software application operable for ... authenticating the user via the unique identification (ID) when the user communicates with the server computer". The Office Action avers that this limitation is taught in Broadhurst [passage 1] reproduced below. (Office Action, Page 5, Paragraph 8, Lines 7,8).

> [Passage 1] In step 104, it is determined whether the user already has a cookie containing a network credential. If there is not yet a cookie one is created in step 106. (Broadhurst, Column 4, Lines 20-23).

Studying this passage, there is nothing in the passage that discloses or suggests authenticating the user via a unique ID. The passage says only that is determined if the user has a cookie with a network credential and if there is no cookie one is created. Notably, the user is not authenticated via a unique ID as recited in claims 11-13.

There really is no reason for Broadhurst's system to authenticate a user via a unique ID because the Broadhurst's cookie stored on the client already contains the network credential. (Broadhurst, Column 4, Lines 20-23 32-37).

Specifically, Broadhurst cookie is formed by appending the identity of a user terminal to a credential that includes a user role. (Broadhurst, Column 4, Lines 28-31). A cryptographic seal of the result is then made. (Broadhurst, Column 4, Line 31). The cookie is given by the web server to web browser (client) ... and stored by the web browser to facilitate access to additional web resources. (Broadhurst, Column 4, Lines 32-37). Thus, the web browser (client) already has a cookie containing the network credential and there is no need for the server to authenticate the client via a unique ID. Broadhurst's server uses the credential to permit access

to the server resources commensurate with the user role that is included in the credential. (Broadhurst, Column 4, Lines 28-31). Since the credential stored on the client contains all of the user's access rights, there is no need to authenticate the user via a unique ID as recited in claims 11-13.

Claim Rejections - 35 U.S.C. §103

Claims 3 and 6

Claims 3 and 6 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Patent No. 6,324,648 to Grantges. Applicant respectfully traverses.

Grantges discloses a computer system for authenticating a user 18 through the use of a client side digital certificate. (Application, Abstract, Column 3, Line 66 – Column 4, Line 4). The digital certificate is sent to a proxy server 34 that checks the certificate to see whether the certificate has been issued by a preapproved certificate authority. (Application, Column 4, Lines 43-48). The proxy server then sends the certificate to a gateway 38 to be authenticated at a more substantive level. (Application, Column 4, Lines 48-55).

Claims 3 and 6 depend from claim 1 and are patentable for the same reasons as claim 1. Grantges like Broadhurst fails to disclose "matching the unique identification (ID) stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers" making claims 3 and 6 patentable over Broadhurst in view of Grantges.

Claims 5 and 8

Claims 5 and 8 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Patent No. 5,764,915 to Heimsoth. Applicant respectfully traverses.

Heimsoth discloses an object oriented protocol interface for establishing a communication path between communication endpoints in a computer network. (Heimsoth, Column 2, Lines 41-43). Heimsoth disclosure is not concerned with matching a client ID with that of a server.

Claims 5 and 8 depend from claim 1 and are patentable for the same reasons as claim 1. Heimseth like Broadhurst is silent regarding "matching unique identification (ID) stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers" making claims 5 and 9 patentable over Broadhurst in view of Heimseth.

Claims 4 and 7

Claims 4 and 7 were rejected under 35 U.S.C. § 103(a), as being unpatentable over Broadhurst in view of U.S. Publication No. 2002/0010776 to Lerner. Applicant respectfully traverses.

Lerner's publication is directed towards an integrated distributed shared services architecture. (Lerner, Paragraph 26). Lerner uses a cookie based architecture to provide this service. (Lerner, Paragraph 33). Browser cookies are passed over the internet from one application to another through browser redirects. (Lerner Paragraph 37). Lerner purports that this allows small amounts of user information to be passed from one server to another in authentication process. (Lerner, Paragraph 37).

Claims 4 and 7 depend from claim 1 and are patentable for the same reasons as claim 1. Lerner like Broadhurst fails to disclose matching unique identification (ID) stored on the client to that stored either on the first or other servers when the user correspondingly communicates with either the first or other servers" making claims 4 and 7 patentable over Broadhurst in view of Lerner.

Newly Drafted Claims

Claims 14-20 are newly drafted and recite embodiments of the invention previously disclosed. Support for each of these claims may be found in the originally filed application as indicated below.

Claim 14 recites the method of claim 1 wherein the step of creating a unique identification for the user includes generating a random number. (Application, Page 5, Lines 12-

14).

Claim 15 recites the method of claim 1 wherein in the step of communicating the unique identification to the client and other servers the unique identification is not embedded in a cookie. (Application, Page 7 Line 24 – Page 8 Line 1).

Claim 16 recites the method of claim 1 wherein in the step of communicating the unique identification to the client and other servers the unique identification is not embedded in a cookie. (Application, Page 7 Line 24 – Page 8 Line 1).

Claim 17 recites the method of claim 1 wherein the step of communicating user information to a first server from a client the user information includes a name, address and phone number. (Application, Page 6 Line 16-19).

Claim 18 recites the computer network system of claim 11 wherein the client software application does not store cookies. (Application, Page 7 Line 24 – Page 8 Line 1).

Claim 19 recites the computer network of claim 13 wherein the at least one additional server computer running is operably connected to the server computer through a business network link. (Application, Figure 1, Page 4, Line 2).

Claim 20 recites the computer network of claim 19 further comprising a firewall between the one server computer and the client computer. (Application, Figure 1, Page 4, Line 2).

Claims 14-20 depend from claims 1, 10 and 11 and are patentable for the same reasons as claims 1, 10 and 11 as explained above.

CONCLUSION

Applicants submit that all pending claims are now in condition for allowance and a notice of allowance is respectfully requested.

Respectfully submitted,

Dated: Jan 24, 2008

/James K. O'Hare/
James K. O'Hare
Reg. No. 56,574

Address all correspondence to:
FITCH, EVEN, TABIN & FLANNERY
120 So. LaSalle Street, Ste. 1600
Chicago, IL 60603

Direct telephone inquiries to:
Thomas F. Lebens
120 So. LaSalle Street, Ste. 1600
Chicago, IL 60603
(805) 781-2865